UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ELLIOT BROIDY and BROIDY CAPITAL MANAGEMENT, LLC, Plaintiffs, —*v.*— GLOBAL RISK ADVISORS LLC, GRA MAVEN LLC, GRA QUANTUM LLC, GLOBAL RISK ADVISORS EMEA LIMITED, and KEVIN CHALKER, Defendants.	19 Civ. 11861 JURY TRIAL DEMANDED

COMPLAINT

Plaintiffs Elliott Broidy and Broidy Capital Management ("BCM"), by and through their undersigned counsel, bring this action against Defendants Global Risk Advisors LLC ("GRA LLC"), GRA Maven LLC ("GRA Maven"), GRA Quantum LLC, Global Risk Advisors EMEA Limited and Kevin Chalker (collectively, "GRA"), and allege as follows.

INTRODUCTION

1. Plaintiff Elliott Broidy is a businessman who has long been a critic of countries like the State of Qatar ("Qatar") that fund and harbor terrorists. Mr. Broidy's work has helped bring significant public condemnation to Qatar, including from the President of the United States and several Congressional leaders, for Qatar's support of al Qaeda, the Muslim Brotherhood and a host of other terrorist organizations. In an effort to retaliate against and silence Mr. Broidy, Qatar hired its go-to firm for underhanded cyber-operations, Defendant GRA, to unlawfully hack into Mr. Broidy's emails and into his company's servers to steal private communications, business documents, and other material. Curated selections of the stolen material were then

leaked to the media by a group of public relations and media professionals, who were acting in concert with GRA and who are being sued in a parallel action in the District of Columbia.

2. The leaks were designed to discredit and cause maximum damage to Mr. Broidy and to his company, Plaintiff BCM. For example, the leaks created the false impression, repeated in multiple media stories, that Mr. Broidy was a target of special counsel Robert Mueller's investigation, when in fact he was never contacted by Mr. Mueller's office and his name appears nowhere in the Mueller Report. The overarching purpose of Defendants' scheme was stated plainly by one of Qatar's henchmen in a WhatsApp message: to "make Broidy go away." When a negative story was published in the *Wall Street Journal* based on the stolen material, another WhatsApp message celebrated with the simple statement, "He's finished."

3. Mr. Broidy and BCM are not finished. They have not gone away, nor will they. They have hired experts to conduct forensic investigations into the unlawful hacks, and have gained additional information even before merits discovery. The investigation is ongoing. The information obtained to date reveals GRA's involvement in the unlawful hacking scheme, for which Mr. Broidy and BCM now seek to hold accountable GRA, including its CEO and operative Kevin Chalker.

4. The investigation has also revealed that GRA's cyber-attack against Mr. Broidy and BCM is part of larger international criminal enterprise and conspiracy ("the Qatari Criminal Enterprise"). The Qatari Criminal Enterprise is a dark-money espionage operation designed to enhance Qatar's tainted reputation around the world and tarnish the reputations of those it considers enemies.

5. To that end, the enterprise contracted GRA to plan and conduct various covert operations, including hacking into private, secured computer systems and stealing private

materials to use in influence campaigns designed to threaten, coerce, discredit, or silence Qatar's purported enemies. For example, GRA assisted in hacking critics of the blatant corruption surrounding Qatar's World Cup 2022 bid, including the tainted vote in which Qatar bribed officials to win hosting privileges.

6. Since its start-up in 2010 — the same year the vote as held on Qatar's bid to host the 2022 World Cup — GRA's largest and most lucrative client by far has been Qatar, enabling the nascent company to open multiple affiliates over the past several years, including Defendant Global Risk Advisors EMEA Limited, which serves as the company's office in Doha, Qatar. To earn that level of support from Qatar, GRA has for years employed cyber-attacks to silence Qatar's critics, like Mr. Broidy and BCM.

7. Mr. Broidy and BCM hereby bring several federal and state causes of action to remedy and prevent serious business and property injury by reason of, and invasion of privacy and other harms caused by, GRA's participation in this egregious scheme. Mr. Broidy and BCM are entitled to relief from GRA's unlawful conduct, as described below.

PARTIES

8. Plaintiff Elliott Broidy is a citizen of the United States and the State of California who resides in Beverly Hills, California. He is the Chief Executive Officer and Chairman of BCM. Plaintiff Mr. Broidy is a prominent business and civic leader and philanthropist who has actively served in leadership roles in the Republican Party and Jewish organizations, including the Simon Wiesenthal Center. His advocacy against terrorism and extremism in protection of his country is well known, as is his criticism of Qatar for sponsoring terrorists.

9. Plaintiff BCM is an investment firm. It is a single-member, limited liability company organized under the laws of the State of California with its principal place of business in Los Angeles, California. Mr. Broidy is the sole member of BCM and resides in California.

10. Defendant Kevin Chalker is the founder and, at all times relevant to this Complaint, the Chief Executive Officer of GRA LLC. He is a citizen of the United States and is domiciled in the state of New York. Mr. Chalker has never registered as an agent of the State of Qatar under the Foreign Agents Registration Act ("FARA"). He is a former CIA officer who advertises his former clandestine experience to obtain clients. In addition to his position at GRA LLC, Mr. Chalker is the director of Bernoulli Limited, which appears to be a shell company formed in Gibraltar for the express purpose of receiving millions of dollars in payments from Qatar. Mr. Chalker also holds a position of authority and control over all subsidiaries and affiliates of GRA LLC and serves as a director to additional shell companies associated with 57/63 Line Wall Road, Gibraltar, including but not limited to Line Holdings Limited, Global Risk Advisors EMEA Limited, and Doraville Limited.

11. Defendant GRA LLC is a limited liability company formed under the laws of Delaware, with its primary place of business in New York, New York. GRA LLC has a branch office located at 1140 Connecticut Ave. N.W. Suite 1120, Washington, D.C. 20036-4007. It has not registered as a FARA agent of the State of Qatar.

12. GRA LLC wholly owns (a) Defendant Global Risk Advisors EMEA Limited, a Gibraltar corporation, which began to operate in Doha, Qatar on October 26, 2017; (b) Defendant GRA Maven, a military consulting firm which was founded by Mr. Chalker in 2016 and which is headquartered in Southern Pines, North Carolina; and (c) Defendant GRA Quantum, a full-service cybersecurity company which was founded by Mr. Chalker in 2015, and which maintains an office in New York, New York. Upon information and belief, the foregoing GRA entities were all utilized in the cyber-attacks on Plaintiffs.

JURISDICTION

13. This Court has federal question subject matter jurisdiction pursuant to 28 U.S.C. § 1331. A number of Plaintiffs' claims arise under federal law, including claims under the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*; the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2) and (a)(5); the Digital Millennium Copyright Act, 18 U.S.C. § 1030(a)(2) and (a)(5); the Defend Trade Secrets Act, 18 U.S.C. § 1832(a)(1) and (a)(5); the Economic Espionage Act, 18 U.S.C. § 1831; and the Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1962(c) and § 1964.

14. This Court has supplemental jurisdiction pursuant to 28 U.S.C. § 1367 over Plaintiffs' other claims as they relate to the federal statutory claims in this action and form part of the same case or controversy under Article III of the U.S. Constitution.

15. Additionally, this Court has diversity subject matter jurisdiction pursuant to 28 U.S.C. § 1332 because Plaintiffs and Defendants are from different states and the amount in controversy exceeds $75,000, exclusive of interest and costs.

16. In connection with the transactions, acts, practices and course of business described in this Complaint, Defendants, directly and indirectly, have made use of the means or instrumentalities of interstate commerce, of the mails, or of the means and instruments of transportation or communication in interstate commerce.

17. Defendant Kevin Chalker is a citizen of the United States. Defendant GRA LLC is a company incorporated under the laws of Delaware, with its headquarters located in New York. Defendant GRA Maven is a company incorporated under the laws of Delaware, qualified to do business in New York and maintains an office in New York. Defendant GRA Quantum is a company incorporated under the laws of Delaware, qualified to do business in Utah, and regularly conducts business within the state of New York. Defendant Global Risk Advisors

EMEA Limited is incorporated under the laws of Gibraltar, is qualified to do business in New York, and regularly conducts business within the state of New York. The GRA defendants were at all relevant times acting in concert, as agents of one another and co-conspirators, and with the subsidiaries of GRA LLC serving as mere departments of the parent company, performing functions that GRA LLC would otherwise perform on its own. Therefore, they are each subject to the jurisdiction of this Court.

VENUE

18. Venue is proper in this judicial district under 18 U.S.C. § 1965(a) because Defendant GRA LLC has its headquarters in New York City, Defendant GRA Maven maintains an office in New York City, Defendant GRA Quantum maintains an office in New York City, Defendant Kevin Chalker transacts business here, and a substantial part of the events giving rise to the claims occurred in New York City.

19. Alternatively, venue is proper in this judicial district under 28 U.S.C. § 1391(b)(3) because there is no state in which all non-foreign defendants reside, and at least one defendant is subject to personal jurisdiction in New York.

FACTS

20. Defendants coordinated an offensive cyber and information operation against Plaintiffs, including by infiltrating Plaintiffs' computer networks and obtaining unauthorized access to Google email accounts of U.S. persons associated with Plaintiffs. Defendants agreed to provide sophisticated offensive and defensive cyber capabilities to Qatar in order to harm Plaintiffs.

I. DEFENDANTS UNDERTOOK COVERT CYBER OPERATIONS ON BEHALF OF QATAR

21. Defendants have worked with Qatar since at least 2010, performing both defensive and offensive cyber activities designed to isolate, marginalize, and silence those who

criticized Qatar's 2022 World Cup bid. The two aspects of Defendants' engagement (offensive and defensive cyber activities) went hand-in-hand, as developing skills in one domain would improve Defendants' capabilities in the other.

22. Qatar's selection to host the 2022 World cup met with considerable controversy, due to Qatar's ties to terrorism, the corruption surrounding its bid, and Qatar's use of slave labor to construct soccer stadiums and other facilities for the event. In particular, Qatar has been credibly accused of bribery on a massive scale, offering to pay hundreds of millions of dollars to FIFA officials to secure hosting privileges.[1] Qatar's corrupt practices have led to the United States' investigation and prosecution of FIFA, the international governing body of soccer, and its officials.[2] Over sixteen individuals have been convicted of or pleaded guilty to criminal charges related to the corrupt bid.[3]

23. Qatar originally engaged Defendants to undertake covert cyber operations to bolster its image, primarily by intimidating Qatar's critics and generally suppressing criticism of its illegal tactics seeking hosting privileges for the tournament.

24. Upon information and belief, Defendants entered a Memorandum of Understanding with Qatar in March 2012 to funnel over $40 million in payments through Bernoulli Limited, a shell company in Gibraltar, for which Mr. Chalker is listed as a director.

---

[1] Alon Einhorn, *Qatar Offered FIFA $880 Million For Hosting the 2022 World Cup—Report*, The Jerusalem Post (Mar. 10, 2019), https://www.jpost.com/Middle-East/Qatar-offered-FIFA-880-million-for-hosting-the-2022-World-Cup-582998.

[2] Rebecca R. Ruiz, *2 Top Soccer Officials Found Guilty in FIFA Case*, N.Y. Times (Dec. 22, 2017), https://www.nytimes.com/2017/12/22/sports/soccer/fifa-trial.html.

[3] Press Release, U.S. Dep't of Justice, *Sixteen Additional FIFA Officials Indicted for Racketeering Conspiracy and Corruption* (Dec. 3, 2015), https://www.justice.gov/opa/pr/sixteen-additional-fifa-officials-indicted-racketeering-conspiracy-and-corruption.

25. In performance of that contract, GRA began a pattern of deploying its offensive cyber capabilities to silence—or neutralize—those who would challenge Qatar's World Cup hosting privileges.

26. From early in its relationship with Qatar, GRA had designs to expand the relationship with the hopes of managing security related to the 2022 World Cup. Consistent with that goal, GRA soon expanded its paid cyber activities for Qatar to include launching and managing offensive cyber-attacks against Qatar's critics generally, beyond just the World Cup example.

27. As has been publicly reported in *The New York Times* and other media outlets, forensic evidence indicates that Qatar and GRA were likely involved in targeting over 1,000 people and entities via cyber-attacks similar to those deployed against Plaintiffs here, including prominent officials from countries like Egypt and the United Arab Emirates, and an American rabbi, Shmuley Boteach, all of whom are known as outspoken critics of Qatar.[4]

28. In the course of working for Qatar to whitewash its global reputation, Mr. Chalker and GRA communicated and worked regularly with the most senior members of the Qatari government. GRA played a central role in overseeing and managing Qatar's information security and defensive and offensive cyber capabilities.

29. Defendants were paid millions of dollars by Qatar, and/or its affiliated entities, to target its enemies in the United States, including American citizens.

30. In October 2017, when the hack against Plaintiffs was in its planning stages, GRA opened Global Risk Advisors EMEA Limited, organized under the laws of Gibraltar and

[4] David D. Kirkpatrick, *Hackers Went After a Now-Disgraced G.O.P. Fund-Raiser. Now He Is After Them*, N.Y. Times, Sept. 20, 2018, https://www.nytimes.com/2018/09/20/world/middleeast/broidy-trump-hackers-qatar.html.

physically located in Doha, Qatar. The sole purpose of the office is to support GRA's services for Qatar, which is GRA's sole client in the region.

31. Upon information and belief, in October and November 2017, GRA actively recruited new employees and/or contractors within the small community of former U.S. government offensive cyber operatives, and GRA made it clear within that community that they had been retained to conduct or coordinate offensive cyber operations for Qatar.

32. Defendant Mr. Chalker had knowledge of Qatar's hacking scheme and intentionally and purposefully furthered the scheme by hiring cyber operatives and personally conducting and supervising the hackings into Plaintiffs' email servers and computer systems.

33. GRA directed the activities of cyber mercenaries to perform the technical aspects of the illegal intrusion into Plaintiffs' email server and Google LLC's servers, and to work with Qatar's media placement agents to disseminate the curated stolen documents to U.S. news organizations, including individuals or groups associated with known mercenary cyber threat actors.

34. Utilizing its cyber experts and other paid hackers, Defendants organized and perpetrated a cyber-attack against Plaintiffs' computer systems and email servers. Defendants coordinated and supervised the execution of spear phishing emails sent to gain unlawful and unauthorized access to the personal and business accounts of individuals associated with Plaintiffs, used that access to gain unlawful access to Plaintiff BCM's network in California, and then unlawfully accessed Plaintiffs' network and accounts thousands of times over the following months without authorization.

35. Defendants participated in tortious, illegal means to thwart Mr. Broidy's exercise of his First Amendment rights within the United States through a campaign (1) to discredit him

through the press and in the eyes of U.S. government officials, and (2) to interfere in and disrupt Plaintiffs' business relationships. The criminal enterprise and conspiracy relied upon Defendants hacking into Plaintiffs' computer networks, including Plaintiffs' email accounts, which allowed co-conspirators to distribute curated batches of the illegally obtained data to the media in a manner calculated to create a false and injurious image of Mr. Broidy.

II. DEFENDANTS EXECUTE AN UNLAWFUL SCHEME TO HACK PLAINTIFFS' COMPUTER SYSTEMS AND EMAIL SERVERS

36. To discredit and damage Mr. Broidy, Defendants agreed to engage in, and did in fact coordinate and perpetrate, a series of cyber-attacks and other misappropriation of Mr. Broidy's private communications and documents. Defendants were responsible for coordinating and executing the cyber-attacks. Upon information and belief, Mr. Chalker was directing the activity of all the GRA defendants, who were acting in concert with one another, in furtherance of a common objective.

A. Defendants Target Robin Rosenzweig with Spear Phishing Emails

37. Robin Rosenzweig, a U.S. citizen and Mr. Broidy's spouse, serves as legal counsel to Plaintiffs and lives in Beverly Hills. Ms. Rosenzweig has an email account through Gmail, an email service provided by Google LLC ("Google")—a company headquartered in Mountain View, California. Ms. Rosenzweig's Gmail account contains private communications and required at least a username and password for access.

38. On December 27, 2017, Ms. Rosenzweig received an email at her Gmail account that appeared to be a security alert from Google. The email used Google trademarks without the permission of Google, including the Google logo and the Gmail logo. It was sent from a Gmail address and had been disguised to look like an authentic security alert from Google. The email

purported to alert Ms. Rosenzweig that the security on her account had been compromised and that she needed to verify or change her account credentials.

39. When she clicked on the TinyURL link in the email, it directed her to a website that appeared as if it was an authentic Google account login page. TinyURL, based in Pennsylvania, is a redirecting service that provides shortened URLs that redirects a website visitor to the website associated with the longer, masked URL. It is known to be used by hackers and scammers to avoid detection and circumvent spam and malware filters. The vast majority of the "destination" websites—the web pages to which the TinyURL links direct the unsuspecting victims—are hosted by servers based in America or by servers owned by companies with significant operations inside the U.S. The TinyURL address sent to Ms. Rosenzweig was http://tinyurl.com/yaw4jmpn. When the TinyURL link was clicked it redirected Ms. Rosenzweig to a website that contained Google's logo and appeared to be an authentic Google account update page. However, that page was a fraudulent login page that is no longer active. The TinyURL link has since been terminated by TinyURL for being used for spam, fraud, malware, or other illegal activity.

40. That email was one of dozens of "spear phishing" email sent by Defendants. Spear phishing is the use of a fraudulent electronic communication targeted towards a specific individual, organization or business in order to steal data or install malware on a targeted user's computer. These spear phishing emails were designed to gain unauthorized access to Ms. Rosenzweig's Google accounts, which include the full suite of Google's online products, such as Gmail, Google Drive, Google Calendar, Google Contacts, and YouTube. Those accounts contained, among other things, personal emails, business emails, usernames and passwords to access other non-Google accounts, including an account on the computer network of Plaintiff

BCM. Without authorization and in violation of Google's Terms of Service, Defendants used Ms. Rosenzweig's credentials unlawfully to access passwords stored by Ms. Rosenzweig on Google's servers. Gmail Program Policies and Google's Terms of Service expressly prohibit illegal uses as well as sending unauthorized email of any person without their consent.

41. Ms. Rosenzweig's Gmail account was accessed and modified unlawfully and without her consent on or around January 3, 2018, by hackers using the "Mail.ru" service. Defendants modified Ms. Rosenzweig's email account settings so that emails containing "Mail.ru," "viewed," or "alert" were marked as read and moved immediately to her trash folder. Defendants did this to ensure that any legitimate security alerts would not be viewed by Ms. Rosenzweig. "Mail.ru" signifies a Russian email service that publishes an app that can be used by users physically located around the world, including in the United States, to send and receive emails on Mail.ru or other email services like Gmail. Unbeknownst to Ms. Rosenzweig, on January 4, 2018, Ms. Rosenzweig received a true security alert—that went directly to her trash folder—notifying her that a user or users of the Mail.ru app had obtained access to read, send, delete, and manage her Gmail account, all without her awareness or consent. Defendants thereby gained control of Ms. Rosenzweig's Gmail account through Mail.ru. They then used that control to obtain Ms. Rosenzweig's login credentials to BCM's servers.

B. Defendants Target Elliott Broidy's Executive Assistant with Spear Phishing Emails

42. Elliott Broidy's Executive Assistant is a U.S. citizen and resident of Los Angeles, CA. She is an employee of Plaintiff BCM. The Executive Assistant has a private Gmail account, which is used to send and receive personal emails, including private communications, and requires at least a username and password for access.

43. On or around January 14, 2018, just weeks after Ms. Rosenzweig was attacked, Defendants began to send the Executive Assistant spear phishing emails disguised as Google security alerts, which bore Google trademarks used without Google's permission and were sent through Google's Gmail service in violation of Google's Terms of Service and Gmail's Program Policies.

44. One of the fake spear phishing emails contained a fictitious security alert with a picture of the Executive Assistant's face and part of the Executive Assistant's phone number. The email was sent from a misleading Gmail account with the name "Gmail Account" and the email address noreply.user.secure.services@gmail.com, which had been drafted to look like an authentic security alert from Google. The email purported to alert the Executive Assistant that the security on the account had been compromised and that the Executive Assistant needed to verify or change the Google credentials.

45. When the Executive Assistant clicked on the link Defendants placed in the email, it directed the Executive Assistant to an Owly address, which redirected to a website that appeared as if it were an authentic Google account login page.

46. Through their spear phishing attack, Defendants were able to obtain the Executive Assistant's login credentials to BCM's computer systems.

47. Like TinyURL and Bitly, Owly is a redirecting service that provides shortened URLs that redirect a website visitor to the website associated with the longer URL. It is known to be used by hackers and scammers to avoid detection and circumvent spam and malware filters. When the Owly link was clicked, it redirected the Executive Assistant to the following website that contains Google's logo and appeared to be an authentic Google account login page:

http://loms.96.lt/BDHRov58?platform=hootsuite. However, that page was a fake login page that is no longer active.

48. Forensic investigation, however, has determined that one of the unauthorized logins by Defendants to the Executive Assistant's Gmail account was from an identifiable IP address, registered to MIST Harlem, a restaurant and event space located less than a mile from GRA Maven's "Urban Climbing Course."

49. On or about December 27, 2017 Defendants used similar spear phishing methods in an unsuccessful attempt to unlawfully access the Google email account of one of Mr. Broidy's associates, Joel Mowbray.

C. Defendants Infiltrate BCM's Servers

50. Plaintiff BCM has an exchange server physically located in Los Angeles, California, that allows BCM employees to send and receive business and occasional personal emails. Mr. Broidy, his Executive Assistant, and several other employees all have secure email accounts on the BCM server containing private communications that require at least a username and password for access.

51. Defendants' efforts to gain unlawful access to Plaintiff BCM's network in California commenced as early as January 7, 2018. The first successful access was gained on January 16, 2018, just two days after Defendants' successful spear phishing campaign on Mr. Broidy's Executive Assistant.

52. Defendants and fellow conspirators maintained unauthorized and unlawful access to the BCM email server until at least February 25, 2018. During this period, there were thousands of instances of unlawful and unauthorized access to corporate email accounts at Plaintiff BCM, including but not limited to unlawful and unauthorized connections to Mr. Broidy

and his Executive Assistant's email accounts at Plaintiff BCM. Defendants accomplished each of these intrusions with the use of stolen or altered credentials.

53. Defendants' exploitation of BCM's mail server was carried out via thousands of Virtual Private Network and Virtual Private Server (collectively, "VPN") connections that obfuscated the origin of the attack.

54. VPNs route internet communication through additional networks to hide the original source of the connection. Some of these VPN connections occurred via IP addresses assigned to and operated by U.S. companies, who in turn allow third parties to engage in internet-based activity through those servers. This creates privacy for the end user of a VPN, as other servers (such as those hosting websites or mail services, such as Hotmail or Gmail) will only detect the VPN's IP address, but will not know the actual IP address of the person utilizing the VPN. For example, many of the suspicious IP addresses associated with the intrusions into the BCM server were assigned to Micfo LLC, a company headquartered in Charleston, South Carolina, but the IP addresses were leased to companies, such as PureVPN and Secure Internet, LLC, with servers operated across the United States, including in Utah, New Jersey, and Georgia.

55. Based on Plaintiffs' forensic investigation, the spear phishing emails and hacking intrusions used wires to transmit signals across state lines. Approximately 90% of the IP addresses of VPNs involved in the documented, unauthorized access of the BCM system came VPNs operating from U.S.-based VPN servers, with most of the remainder coming from VPNs operating overseas that were previously reported to be favored by criminal actors.

56. Between January 16 and February 25 of 2018, Defendants accessed BCM's mail server, which is known to contain emails, attorney-client privileged information, private

communications, corporate and personal documents, copyrighted material, and contracts, business plans, confidential and sensitive proprietary information, and trade secrets and other intellectual property. Defendants and their co-conspirators had full access to such confidential, sensitive proprietary information and trade secrets and other intellectual property, and stole at least hundreds, and likely thousands, of the documents contained on the server.

57. While the artifacts discovered during Plaintiffs' forensic investigation indicated that the cyber-attack mostly employed VPN technology, Plaintiffs also discovered non-VPN connections many times from within the United States and twice from Qatar.

58. Between February 12 and February 25 of 2018, Defendants and their co-conspirators originated numerous illegal and unauthorized connections into BCM's California-based servers from two VPN addressees in Vermont. These intrusions were not masked by VPNs—even though the connections immediately after the access were routed through VPNs—probably because of momentary human error or because the accessing computer automatically connected to Plaintiff BCM's network before the VPN could be activated. During that period, Defendants and co-conspirators utilized two separate Vermont IP addresses to access Plaintiffs' servers directly at least a dozen times, accounting for 178 connections.

59. These included an IP address associated with a small motel near Killington, Vermont. Intrusions attributed to that address occurred between February 12-24.

60. On February 14, 2018 and February 19, 2018, Defendants executed two unlawful and unauthorized connections into BCM's California server originated from an IP address in Qatar. These two unlawful and unauthorized intrusions were not masked by VPNs—even though the connections immediately before and immediately after the access were routed through VPNs—again, probably because of momentary human error or because the accessing computer

automatically connected to Plaintiff BCM's network before the VPN could be activated. These connections represent suspected unmasked intrusion signals accessing BCM's network from an IP address in Qatar.

D. Defendants Help Review and Package the Stolen Emails for Dissemination and Place Them in the Hands of Third Parties

61. After unlawfully obtaining Plaintiffs' private communications, emails, documents, and intellectual property, Defendants and co-conspirators within the United States converted the stolen materials to PDF files and physical printouts for dissemination to third parties, including journalists. Most of the PDFs disseminated to third parties bear time stamps different from the Pacific Time Zone associated with the original documents—and instead bear time stamps from the Central and Eastern Time Zones of the United States, where Defendants were located at the time that they converted the emails to PDF format.

62. On February 24, 2018, members of the Qatari Criminal Enterprise registered the email address "LA.Confidential@mail.com" through the company 1&1 Internet, Inc., which operates in the United States through offices in Chesterbrook, Pennsylvania. Mail.com provides free email addresses akin to Google's Gmail service. Defendants used this email address to unlawfully deliver Plaintiffs' stolen emails to journalists employed by U.S. media organizations. Defendants and their co-conspirators directed selected third parties, including media members, to this site to get copies of curated sets of the stolen documents.

63. An IP address based in New York, NY, where GRA is headquartered, accessed the "LA.Confidential@mail.com" during this time.

64. Defendants used another IP address traced to the North Carolina Research and Education Network ("NCREN") and a server in Chapel Hill, North Carolina—close to GRA Maven's Southern Pines, North Carolina offices—to deposit the PDF formatted electronic

documents into the "LA.Confidential@mail.com" during this time. NCREN provides broadband infrastructure to various public institutions in North Carolina, and the particular IP address at issue is associated with a "guest" Wi-Fi network at the University of North Carolina. This point of access for the conspirators' email is roughly an hour's drive from GRA Maven's location and from the towns where GRA employees lived at that time.

65. Plaintiffs' stolen emails have also appeared on a website hosted by a U.S. company, Amazon Inc, based in Seattle, Washington, and registered through GoDaddy LLC ("GoDaddy"), which is headquartered in Scottsdale, Arizona. GoDaddy is a domain registrar and web hosting service that sells website domains to users so they may create their own webpage and host websites. Defendants further obfuscated their identity using a registration masking service, Domain by Proxy LLC, which allows a user to replace their own personal information with information belonging to Domain by Proxy LLC for purposes of registration. Domain by Proxy LLC is a company owned by GoDaddy LLC.

66. In some cases, to avoid later detection, Defendants' co-conspirators handed printed out physical PDFs to third parties, including members of the media.

E. Defendants' Attacks on Plaintiffs Are Part of a Pattern of Cyber Attacks Orchestrated by the Qatari Criminal Enterprise

67. These cyber-attacks resemble a pattern of known international attacks by sophisticated, nation-sponsored cyber-hackers. Previous attacks against other victims by these same threat actors have involved similar fake news alerts, malicious Google login pages, email addresses designed to resemble legitimate Google security addresses, falsified two-factor authentication messages, and the use of Mail.ru to control victims' accounts.

68. Mr. Broidy was not the only outspoken critic of Qatar targeted by the hacking scheme. More than one thousand individuals have been victimized by similar hacking intrusions

by the Qatari Criminal Enterprise since at least 2014.[5] The victims range from high-profile figures in government, business, journalism, and human rights advocacy in the United States, Europe, the Middle East, and elsewhere around the world. Dozens of U.S. citizens and organizations have been targeted and injured, including former intelligence officials, former staffers from the Democratic National Committee and the Hillary Clinton Presidential campaign, high-profile political activists opposed to the Assad regime in Syria, and a researcher at a Washington, D.C. think tank currently investigating foreign influence in the 2016 elections. Other targets include FIFA soccer stars, former European defense officials, and hundreds of government leaders and diplomats across the Middle East. The hacking conspiracy also targeted users of "@un.org" email addresses, journalists, and lobbyists.

69. In particular, one other prominent critic of Qatar targeted by the hacking conspiracy was American Rabbi Shmuley Boteach.[6] Upon information and belief, another target was a close associate of President Trump in the White House.

70. These numerous cyber-attacks have extended over years and represent a pattern of unlawfully accessing victims' computer systems to extract private information, extortion material, or other items of value.

71. In addition to cyber-attacks in which information was stolen, Qatar has used unlawful and unauthorized access to computer systems to plant documents that would appear to incriminate their purported enemies.

---

[5] *See* Eli Lake, *Russian Hackers Aren't the Only Ones to Worry About*, Bloomberg (Sept 18, 2018), https://www.bloomberg.com/opinion/articles/2018-09-18/russian-hackers-aren-t-the-only-ones-to-worry-about.

[6] *See* Shmuley Boteach, *Qatar's War to Destroy Pro-Israel Jews*, *The Jerusalem Post* (Oct. 8, 2018), https://www.jpost.com/Opinion/Qatars-war-to-destroy-pro-Israel-Jews-568942.

72. These cyber-attacks are all part of the pattern of racketeering activity in which the Qatari conspirators have engaged.

73. The cyber-attacks also coincide with Defendants' growing relationship with Qatar, its most important client.

F. Defendants' Co-Conspirators Place the Stolen Emails with Media Outlets

74. Once Defendants successfully stole Plaintiffs' documents, they transmitted them to other members of the Qatari Criminal Enterprise, including Nicholas Muzin, Joseph Allaham, and Gregory Howard.

75. Through all times relevant to this Complaint, Nicolas D. Muzin was the Chief Executive Officer of Stonington Strategies LLC, a public relations and lobbying firm incorporated under the laws of Delaware, and a political lobbyist who signed FARA documents on behalf of Stonington as a registered foreign agent of the State of Qatar. On August 24, 2017, he was retained by the State of Qatar for "consulting services." Stonington Strategies has been reorganized into Stonington Global LLC, whose website states that "[i]n launching the new firm, Nick Muzin & his team plan to build on their success representing the State of Qatar."

76. Joseph Allaham was the co-founder of Stonington Strategies, where he served as partner for all times relevant to this Complaint. He has worked for Qatar, originally as an unregistered foreign agent until he belatedly filed a registration statement under FARA on June 15, 2018, in response to a subpoena from Plaintiffs in a related action. He reported that Qatar paid him $1.45 million in October 2017, at almost the same time that Blue Fort PR paid Stonington $3.9 million.[7]

[7] Stonington registered on September 3, 2017, under FARA as a foreign agent providing "strategic communications" for the State of Qatar. Stonington originally was retained to provide these services for $50,000 per month. On November 1, 2017, shortly before the hacks on Plaintiff's computers began, Qatar increased the amount to $300,000 per month. This six-fold

77. Gregory Howard is a media placement expert who in 2017 and 2018 worked as a Vice President and Senior Media Strategist at the firm of Conover & Gould ("Conover"), based in Washington, DC. From July 2017 until January 18, 2018, Gregory Howard was a registered foreign agent of Qatar through Conover. Beginning on May 10, 2018, Mr. Howard worked in Washington, DC, as Vice President of Mercury Public Affairs, a public strategy firm, which he left in April 2019. In each of his positions, Mr. Howard worked as a media placement strategist for Qatar.

78. Mr. Allaham wrote to Mr. Muzin on WhatsApp on March 13, 2018, that a former U.N. official working under contract with the Qatari government, Jamal Benomar, had gone to Qatar prior to the date of the message "to get the emails. That what [*sic*] I think he was doing there [in Qatar]." Mr. Muzin responded by referencing Mr. Broidy by name.

G. The Qatari Criminal Enterprise Coordinates a Smear Campaign Against Mr. Broidy Using Hacked Documents

1. Mr. Howard Places Media Stories Using the Hacked Documents

79. During the relevant time period, Gregory Howard had extensive contacts with both members of the Qatari Criminal Enterprise and reporters working on stories about Mr. Broidy that were based on the materials stolen from Plaintiffs' computer systems and servers. The volume and timing of these contacts show that Mr. Howard was acting in concert with the Qatari Criminal Enterprise during this period.

80. Mr. Howard's phone records show that he orchestrated a sophisticated media and distribution campaign to place information illegally obtained from the hacking in the hands of journalists, media organizations, and public relations professionals.

---

pay raise was in addition to $3.9 million paid to Stonington within three weeks, from late October to mid-November 2017, by Qatari front group Blue Fort PR.

81. Mr. Howard's phone calls following the hacking showed that he was in close and frequent communication with journalists in the early months of 2018 before they began publishing stories that relied on information stolen from Plaintiffs' computer systems and servers. In some instances, Mr. Howard communicated with journalists weeks before they published these articles. The intensity of those contacts often increased in the days prior to publication. During this same period, Mr. Howard closely communicated with public relations experts, research groups, and registered agents of Qatar to coordinate the media disinformation campaign against Mr. Broidy.

82. Starting on January 7, 2018, three days after the first successful spear phishing intrusion, Mr. Howard engaged in a flurry of calls with outside public relations professionals, his then-colleagues at Conover & Gould, and Diogenes Group Research ("Diogenes"), a Florida-based research and graphic design company.

83. From January 18 through May 22 of 2018, Mr. Howard participated in more than two hundred phone calls with reporters who contributed to stories regarding Mr. Broidy and Qatar or regularly covered Qatari-related issues. These included extensive, and at times, almost daily calls with now-former Associated Press ("AP") reporter Tom LoBianco, all before the time he authored several stories regarding Mr. Broidy in March and May 2018 based on the contents of Mr. Broidy's hacked emails. In addition, Mr. Howard conducted more than a dozen calls with the *New York Times*, *McClatchy*, the *Wall Street Journal*, and the *Washington Post*, all of which were focusing on stories regarding Mr. Broidy's hacked emails.

84. On February 21, 2018, Mr. Howard engaged in a call lasting over 40 minutes with a reporter in the Washington, DC office of the *New York Times*. Later that day, Mr. Howard received a call from an unknown individual located in the *New York Times* Washington bureau.

Just under two hours later, Mr. Howard called the direct dial office phone number of the *New York Times*' lead investigative reporter, Mark Mazzetti.

85. At the time, the *New York Times* was researching the story about Mr. Broidy and George Nader that would be published on March 3, 2018. Mr. Mazzetti was the lead author of the piece. This story relied significantly on the material unlawfully stolen from Plaintiffs.

86. In the late morning on March 2, 2018, in the early stages of media inquiries based on the hacked emails and the day before the first such story in the *New York Times*, Mr. Howard exchanged two calls with Diogenes, the second of which lasted over 9 minutes. Mr. Howard later had a call lasting over 15 minutes with a reporter at the Washington, DC office of the *New York Times*.

87. On March 23, 2018—three days before the AP published an article based on Mr. Broidy's emails—Mr. LoBianco, one of the authors of the piece, called Mr. Howard three times in less than an hour, with these calls lasting nearly 40 minutes total. Less than thirty minutes after that final call ended between Mr. LoBianco and Mr. Howard, Mr. LoBianco emailed the first and only batch of hacked emails that his outlet provided to Mr. Broidy's associates before AP published its March 26 article.

88. In the two weeks prior to the release of this article, Mr. Howard had multiple phone calls every day with Mr. LoBianco, the duration totaling almost seven hours. Before March 12, 2018, Mr. Howard's phone records show no contacts with Mr. LoBianco. Over the next two months, however, Mr. Howard continued to be in extensive, and at times, almost daily contact with Mr. LoBianco, as Mr. LoBianco continued to pursue stories based on Mr. Broidy's stolen emails.

89. On March 24, 2018, Mr. LoBianco and Mr. Howard had at least two conversations, lasting a total of over 30 minutes, and they exchanged two more calls the next day, March 25.

90. On March 26, 2018, the AP published an article by Mr. LoBianco and other staff, based on documents stolen from the cyberattack. The article noted that "[s]cores of Mr. Broidy's emails and documents have leaked to news organizations," but did not indicate that the stolen materials were provided by an "anonymous" source.

91. On March 28, 2018, Mr. Howard spoke for more than 20 minutes with *New York Times* reporter Ken Vogel. The next day, Vogel retweeted a since-corrected *Newsweek* story, and made disparaging remarks about Mr. Broidy. Vogel later deleted the tweet.

92. On April 27, 2018, Mr. LoBianco notified an associate of Mr. Broidy, "We got a new batch of emails." In the days leading up to that message, Mr. LoBianco and Mr. Howard exchanged at least four phone calls between April 18 and April 24, which totaled approximately 45 minutes. On May 2, 2018, Mr. Howard called Mr. LoBianco at least once early that evening.

93. On May 8, 2018, Mr. Howard and Mr. LoBianco exchanged calls, with at least one call lasting more than nine minutes, followed by at least one call between the pair on each of the next two days.

94. On May 11, 2018, Mr. LoBianco emailed to Mr. Broidy's representatives a first batch of images of Mr. Broidy's hacked emails upon which he planned to report for what became his second article in the AP based on Mr. Broidy's emails. That article was published on May 21, 2018.

95. On May 11, 2018, Mr. Howard and Mr. LoBianco had at least two conversations that afternoon, hours before Mr. LoBianco sent to Mr. Broidy's representatives copies of the hacked emails.

96. The final batch of hacked emails that Mr. LoBianco provided to Mr. Broidy's representatives was sent on May 18, 2018.

97. In total, between March 12 and May 22, 2018, Mr. Howard and Mr. LoBianco logged nearly fifteen hours of time over the phone. During the entire time Mr. Howard was in conversations with Mr. LoBianco, Mr. Howard was not registered as a foreign agent representing the Qatari interests.

98. In Conover & Gould's FARA Supplemental Statement filed on February 28, 2018, the firm claimed that it terminated its work on behalf of Qatar on January 18, 2018—two days after the first successful breach of BCM's computer systems and servers. According to that Supplemental Statement, the last communication Mr. Howard had with a media entity on behalf of Qatar occurred on December 15, 2017, almost a month before the supposed termination date of Conover & Gould's representation of Qatar.

99. Mr. Howard did not register again as a foreign agent of any country until May 10, 2018, when he worked at Mercury. According to Mercury's September 7, 2017 contract-modification FARA filing, Mercury's work on behalf of Qatar was focused on media relations, its monthly pay from Qatar increased to $120,000 that year, and its work would be overseen by the "Government Communications Office of the State of Qatar."

100. Before assuming his role at his firm Mercury on May 10, 2018, Mr. Howard had approximately two dozen calls with members of the firm, almost all of which came at key times in the planning or execution of the media dissemination phase of the conspiracy. Several of the

phone lines he contacted are registered to registered Qatari agents Katherine Lewis and Jennifer Kaufmann, as well as Molly Toomey, whose bio on the Mercury website states that she "[l]ed international PR" for a "$1 billion" project financed by Qatar Investment Authority.

101. Although Mercury has acted for years as a FARA-registered agent of Qatar, Mr. Howard's Short Form registration submitted in May 2018 as an employee of Mercury omitted Qatar as one of the foreign principal clients whose interests he was registering to represent. Mercury's FARA filings indicate that Mr. Howard's first foreign principal-related media interaction happened on May 22, precisely one day after the May 21 publication of Mr. LoBianco's second and final AP story on Mr. Broidy.

2. Mr. Muzin and Mr. Allaham Celebrate Their Conspiracy and Share Advance Notice of Media Accounts of Plaintiffs Based on the Hacked Emails

102. Mr. Muzin and Mr. Allaham's text messages demonstrate their direct and prior knowledge of the hacking and their knowing use of stolen documents.

103. During the time of the cyberattacks against Mr. Broidy, Mr. Muzin was in Qatar.

104. On January 25, 2018, shortly after the successful hacking of BCM began, Mr. Muzin sent Mr. Allaham a message on WhatsApp, stating, "It's very good. . . . We got the press going after Mr. Broidy. I emailed you." Mr. Muzin and Mr. Allaham shared stolen information gained from the cyberattack with journalists in order to convince them to "go[] after Mr. Broidy."

105. On January 25, 2018, prior to the first public reports in the United States of materials stolen from Plaintiffs, Ben Wieder, a reporter for *McClatchy*, a Washington, DC publication focused on politics, emailed Mr. Muzin to tell him, "I'm working on a story about Elliott Broidy and was hoping to talk." Mr. Muzin, who at the time was still in Qatar after having flown there within a few days of the hackers' first successful breach into the BCM

servers and computer systems, forwarded this message to Mr. Allaham and commented, "Time to rock." Less than an hour after sending the email to Mr. Muzin, Mr. Wieder called Mr. Howard, and they spoke for more than 10 minutes. Mr. Wieder would go on to write extensively about Mr. Broidy on the basis of carefully curated emails and other documents stolen from Mr. Broidy's servers.

106. On March 1, 2018, the contents of emails stolen from Plaintiffs' computer accounts and servers appeared for the first time in media accounts, in a *Wall Street Journal* article that noted that it was based on "a cache of emails from Mr. Broidy's and his wife's email accounts that were provided to the Journal."

107. Mr. Muzin shared the *Wall Street Journal* article with Mr. Allaham over WhatsApp that same day. Mr. Muzin then commented, "He's finished."

108. Additional emails stolen from BCM's accounts and servers were published or reported on in other media outlets including the *Huffington Post* on March 2, 2018, which reported based on "[e]mails and documents an anonymous group leaked to HuffPost," as well as the BBC on March 5, 2018.

109. Mr. Muzin admitted to having foreknowledge of impending media stories about Mr. Broidy based upon the hacked material. On February 28, 2018, Mr. Muzin called Joel Mowbray and informed him that the *New York Times* was about to publish a story about Mr. Broidy and George Nader, saying that he received this information from his "media guy." The article was not published until March 3.

110. Upon information and belief, Mr. Muzin's "media guy" is Mr. Howard.

111. On March 13, 2018, Mr. Muzin remarked to Mr. Allaham via WhatsApp that recent news stories about Mr. Broidy have "[p]ut[] him in [M]ueller['s] crosshairs." This

communication demonstrates one of the central goals of the Qatari Criminal Enterprise—to portray Mr. Broidy as a target of special counsel Robert Mueller's investigation.

112. On March 26, 2018, *McClatchy* published a story that discussed Mr. Broidy, authored by Ben Wieder. It was only one of a series of articles hostile to Mr. Broidy authored by Mr. Wieder following contact with Mr. Muzin and Mr. Howard, who also had extensive communications with Mr. Wieder's editor Viveca Novak and his frequent writing collaborator, Peter Stone.

113. On March 14, 2018, Mr. Muzin told Mr. Allaham on WhatsApp that he'd "get some intel about the Mr. Broidy event soon." This comment likely refers to a March 13, 2018, Republican fundraiser headlined by the President of the United States, for which Mr. Broidy had been listed as an event host.

114. The next day, on March 15, 2018, Mr. Muzin exclaimed to Mr. Allaham, via WhatsApp, "Elliott Broidy was not at the fundraiser!" Mr. Muzin and Mr. Allaham were excited at the prospect of furthering their objective of politically damaging Mr. Broidy.

115. Ten days later, on March 25, 2018, a front-page story in the *New York Times* reported extensively on Mr. Broidy's fundraising and business activities. The story reported that Mr. Broidy had agreed not to attend the March 13 fundraiser. The story was based, in part, on "[h]undreds of pages of Mr. Broidy's emails, proposals and contracts" received from what the *Times* euphemistically termed "an anonymous group critical of Mr. Broidy's advocacy of American foreign policies in the Middle East." This "anonymous group" is the Qatari Criminal Enterprise.

116. On March 21, 2018, the *New York Times* published a front-page article noting that an "anonymous group critical of Mr. Broidy's advocacy of American foreign policies in the

Middle East" has been distributing "documents, which included emails, business proposals and contracts," belonging to Plaintiffs. On March 23, 2018, *Bloomberg* published an article about Mr. Broidy, which noted that it had "received two separate documents this week purporting to be versions" of materials belonging to Mr. Broidy.

117. James Courtovich of Sphere Consulting, who is a registered agent of Qatar had more than a dozen known calls and text messages with conspirators between February and April of 2018, including several texts on April 13.

118. The following day, April 14, 2018, Mr. Courtovich met with Julie Bykowicz of the *Wall Street Journal*, according to his FARA Supplemental Statement filed on October 30, 2018. On April 18, 2018, the *Wall Street Journal*'s Bradley Hope, a colleague and frequent collaborator of Ms. Bykowicz, reached out to Mr. Broidy's representatives with a lengthy set of questions relating to a new, previously unreleased batch of hacked emails. The *Wall Street Journal* ultimately did not publish the story.

119. On May 1, 2018, Mr. Courtovich emailed the *Wall Street Journal*'s Rebecca Ballhaus, according to his FARA filing. The next day, on May 2, Ms. Ballhaus contacted Mr. Broidy's representatives asking questions for an intended "profile," which would be substantially based on the contents of Mr. Broidy's hacked emails. The *Wall Street Journal* ultimately did not publish the story.

120. On May 4, 2018, Mr. Muzin contacted Mr. Allaham via WhatsApp. Mr. Muzin told Mr. Allaham that "our new friends can make Broidy go away altogether."

121. On October 26, 2018, Stonington Strategies LLC, filed a FARA supplemental statement indicating that Mr. Muzin terminated his representation of Qatar "[n]o later than

August 21, 2018." Mr. Muzin has failed to disclose any payment he received from Qatar after February 6, 2018, or payment for any activities described above.

122. Media outlets in the United States and abroad have continued to publish—and to threatened to publish—materials stolen from Plaintiffs well into 2019. Plaintiffs continue to receive numerous press inquiries concerning such materials.

123. All of this evidence, obtained through limited discovery and Plaintiffs' investigation to date, is highly probative of the fact that Mr. Muzin, Mr. Allaham, and Mr. Howard had received and were knowingly using the stolen emails—emails that they never would have been able to access without the assistance of Defendants. It is likely that after a reasonable opportunity for further investigation or discovery, Plaintiffs would produce additional evidentiary support to establish these allegations.

III. PLAINTIFFS BRING LAWSUITS AGAINST INDIVIDUAL MEMBERS OF THE QATARI CRIMINAL ENTERPRISE

124. On March 19, 2018, Mr. Broidy and BCM, through counsel, formally requested that Qatar take appropriate action to halt the attacks on Plaintiffs' emails, documents, and data, to stop Defendants from disseminating Plaintiffs' emails, documents, and data, and/or to assist Plaintiffs in halting dissemination if the hack had been conducted by a rogue agent of Qatar.

125. When Qatar failed to respond to Plaintiffs' request, Mr. Broidy and BCM filed suit in the United States District Court for the Central District of California against, Qatar, Defendants, and several other individuals and entities responsible for the hacking scheme on March 26, 2018. On May 4, 2018, the parties stipulated to a stay to permit limited discovery. In conducting this discovery, Plaintiffs were able to uncover the phone records for some of the co-conspirators and others, as well as some WhatsApp chats among Mr. Muzin, Mr. Allaham, and other conspirators. Plaintiffs have used this narrow opportunity for discovery to amply

substantiate the above allegations. However, this discovery was limited to establishing jurisdiction in that case, and did not reach the merits of any of Plaintiffs' claims. The district court dismissed the lawsuit against Qatar on grounds of foreign sovereign immunity, and dismissed all other served defendants for lack of personal jurisdiction. The court did not reach the merits of any claims, and its decision dismissing Qatar is currently under appeal.

126. On July 23, 2018, Plaintiffs also filed suit in the United States District Court for the Southern District of New York against Jamal Benomar. The district court dismissed the case without permitting any jurisdictional discovery, on grounds of diplomatic immunity. The district court did not reach the merits of any of Plaintiffs' claims.

127. On January 24, 2019, Plaintiffs filed suit against Nicholas Muzin, Joseph Allaham, Gregory Howard, and Stonington Strategies. *See Broidy Capital Mgmt. v. Muzin et al.*, No. 19-cv-00150 (D.D.C. filed Jan. 24, 2019) (Friedrich, J.). This suit is currently pending before the United States District Court for the District of Columbia. That pending litigation shares a common nucleus of operative facts with this Complaint, and the allegations, and Counts in this Complaint overlap substantially with the First Amended Complaint filed in that matter.

CAUSES OF ACTION

COUNT ONE

Stored Communications Act
18 U.S.C. § 2701 *et seq.*

128. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

129. The Stored Communications Act imposes criminal penalties on "whoever . . . intentionally accesses without authorization a facility through which an electronic communication service is provided." 18 U.S.C. § 2701(a)(1).

130. The Act also provides that "a person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity" damages, along with equitable and declaratory relief. *Id.* § 2707.

131. Plaintiffs are "persons" within the meaning of 18 U.S.C. §§ 2510(6) and 2707(a).

132. Defendants are directly liable under the SCA for conducting and supervising the hacking of Plaintiffs' email servers and computer systems.

133. Defendants willfully and intentionally accessed without authorization a facility through which an electronic communication service is provided, namely, BCM's computer systems, including its email servers, as well as Google's servers, thereby obtaining access to wire or electronic communications while they were in electronic storage in such systems, in violation of 18 U.S.C. § 2701(a).

134. The cyber-attack was a willful, flagrant, and intentional violation of the Stored Communications Act. Defendants used VPN and other tools to mask their cyber intrusions and avoid detection, thereby showing sophistication and consciousness of guilt. Defendants unlawfully and without authorization accessed Plaintiffs' computer systems and email servers thousands of times over a period of almost two months, in a sustained cyber-attack.

135. As a result of Defendants' conduct, Plaintiffs have suffered damages, including, but not limited to, loss of consumer goodwill; harm to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets, confidential business information, and other intellectual property; and harm to Plaintiffs' business, in an amount to be proven at trial. As provided for in 18 U.S.C. § 2707, Plaintiffs are entitled to an award of the greater of the

actual damages suffered or the statutory damages, punitive damages, attorneys' fees and other costs of this action, and appropriate equitable relief.

136. Defendants' conduct has caused, and will continue to cause, Plaintiffs irreparable injury, including loss of consumer goodwill, an increased risk of further theft, and an increased risk of harassment. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting Defendants from engaging in any further cyber-attacks or committing the conduct described in this Cause of Action.

COUNT TWO

Computer Fraud and Abuse Act
18 U.S.C. § 1030(a)(2) and (a)(5)

137. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

138. The Computer Fraud and Abuse Act creates a cause of action against whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2).

139. The Act also creates a cause of action against whoever "(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss." *Id.* § 1030(a)(5).

140. The Act also creates a cause of action against "[w]hoever conspires to commit or attempts to commit an offense under subsection (a) of this section." *Id.* § 1030(b).

141. A "protected computer" is one that "is used in or affecting interstate or foreign commerce or communication." *Id.* § 1030(e)(2)(B).

142. BCM's computer systems and email servers are used in and affect interstate and foreign commerce or communication and are therefore "protected computers."

143. Defendants breached Plaintiffs' protected email servers and computer systems thousands of times over a period of almost two months, in a sustained cyber-attack.

144. Defendants intentionally, unlawfully, and without authorization accessed Plaintiffs' computer systems and email servers thousands of times over a period of almost two months, in a sustained cyber-attack. Defendants intentionally conspired to cause damage to BCM's protected computers through the attack.

145. Defendants intentionally accessed or caused to be accessed Plaintiffs' servers, and emails and documents physically located on those servers, at BCM's offices, as well as Google servers, specifically by accessing or causing to be accessed accounts associated with Mr. Broidy and other BCM employees.

146. Defendants accessed "protected computers," defined by 18 U.S.C. § 1030(e)(2)(B) as computers "used in or affecting interstate or foreign commerce or communication." They knowingly caused the transmission of a program, information, code, or command, and as a result, intentionally causes damage without authorization, to BCM's protected computers.

147. Defendants willfully and intentionally accessed the email accounts of, at least, Robin Rosenzweig and Mr. Broidy's Executive Assistant by transmitting fake spear phishing emails that stole their login credentials, and thereafter, beginning on or about January 16, 2018,

accessed BCM's servers without authorization. They accessed emails and documents physically located on those servers, including the accounts of Mr. Broidy and other BCM employees.

148. Defendants also implemented identifiable obfuscation techniques, such as VPN, to engage in ultimately unsuccessful efforts to hide the origin of their spear phishing attacks and unauthorized access to Plaintiffs' servers, and emails and documents physically located on those servers and the servers of Google.

149. As a direct and proximate result of the actions of Defendants and their co-conspirators, Plaintiffs suffered damage, including harm to the integrity and availability of their servers, and to emails and documents physically located on those servers.

150. As a direct and proximate result of the actions of Defendants and their co-conspirators, Plaintiffs also suffered loss, including, but not limited to, damages resulting from loss of consumer goodwill; harm to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets, confidential business information, and other intellectual property; the investigation costs associated with identifying the cyber-attacks and repairing the integrity of Plaintiffs' servers after the attacks, including by hiring forensic investigators and data security experts, and attorneys, among other losses, in an amount to be proven at trial, but in any event, in excess of $75,000, exclusive of interest and costs.

151. Defendants intentionally and willfully caused such damage to Plaintiffs.

152. Defendants' conduct has caused, and will continue to cause Plaintiffs irreparable injury, including loss of consumer goodwill, an increased risk of further theft, and an increased risk of harassment. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting Defendants from engaging in the conduct described in the Cause of Action.

COUNT THREE

Violation of the Digital Millennium Copyright Act
17 U.S.C. § 1201 *et seq.*

153. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

154. Federal law provides that "[n]o person shall circumvent a technological measure that effectively controls access to a work protected" under the copyright laws. 17 U.S.C. § 1201.

155. Plaintiffs' computer networks and files contained information subject to protection under the copyright laws of the United States. Defendants willfully accessed these materials illegally and without authorization. These materials included, but were not limited to, presentations, proprietary business plans and proposals, and strategic correspondence.

156. Access to the copyrighted material contained on Plaintiffs' computer networks and email accounts was controlled by technological measures, including firewalls, antivirus software, and measures restricting access to users with valid credentials and passwords.

157. Defendants conducted a targeted attack to circumvent these technological measures by stealing usernames and passwords from authorized users. Defendants sent spear phishing emails containing links to malicious websites designed to trick users into providing usernames and passwords. Defendants used the information they obtained from their spear phishing attacks to gain unauthorized access to Plaintiffs' computer networks and email accounts.

158. Defendants' conduct caused Plaintiffs significant damages, including, but not limited to, damage resulting from harm to Plaintiffs' computers, loss in the value of Plaintiffs' proprietary business information, and harm to their business interest.

159. As a result, Plaintiffs are entitled to the greater of their actual damages or statutory damages as provided by 17 U.S.C. § 1203, in an amount to be proven at trial. Plaintiffs are further entitled to attorneys' fees and costs as provided by 17 U.S.C. § 1203.

160. Defendants' conduct has caused, and will continue to cause Plaintiffs irreparable injury, including loss of customer, goodwill, an increased risk of further theft, the costs of securing Plaintiffs' computer systems and email servers among other injuries to be proven at trial. Such injury cannot be compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting Defendants from engaging in the conduct described in the Cause of Action.

COUNT FOUR

Misappropriation of Trade Secrets (18 U.S.C. §§ 1831, 1832, 1836)

161. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

162. Federal law creates a cause of action against "[w]hoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly . . . steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains" trade secrets. 18 U.S.C. § 1832(a)(1).

163. Federal law imposes criminal penalties on "whoever . . . conspires with one or more other persons" to violate § 1832(a)(1). *See id.* § 1832(a)(5).

164. Federal law also creates a cause of action against "[w]hoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign

agent, knowingly—(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret." *Id.* § 1831(a)(1).

165. Federal law imposes penalties on "[w]hoever . . . conspires with one or more other persons to commit" the offense listed in § 1831(a)(1). *See id.* § 1831(a)(5).

166. "An owner of a trade secret that is misappropriated may bring a civil action. . . if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." *Id.* § 1836(b)(1). The owner may seek remedies including, *inter alia*, injunctive relief and "damages for actual loss caused by the misappropriation of the trade secret." *Id.* § 1836(b)(3)(A-B).

167. The BCM computer systems and email servers stored trade secrets, including but not limited to highly confidential business plans and proposals; research supporting those plans and proposals, including cost proposals and service projections; information concerning business strategies and opportunities; and contacts for important business relationships. These trade secrets are of substantial value to Plaintiffs, as will be proven at trial.

168. BCM stored trade secrets that were used in interstate and foreign commerce. Plaintiffs have taken and continue to take reasonable measures to keep this information secret. For example, Plaintiffs have always maintained their information on secured servers that are protected by passwords, firewalls, and antivirus software.

169. Moreover, Plaintiffs' emails contained confidential information involving contracts, business proposals, and cost estimates involving Mr. Broidy's company and its clients. These contracts, proposals, and estimates contained sensitive information about Mr. Broidy's clients and his company's confidential technology and methods.

170. Plaintiffs' trade secrets derive independent actual and potential economic value from not being generally known or available to the public or other persons who can obtain economic value from their disclosure or use.

171. Plaintiffs' trade secrets have significant value, resulting from significant investment of time and resources.

172. Plaintiffs have made, and continue to make, efforts that are reasonable under the circumstances to maintain the secrecy of their trade secrets.

173. Defendants unlawfully conspired to take, appropriate, and obtain Plaintiffs' trade secrets without authorization, by means of a cyber-attack against Plaintiffs. Defendants knew that BCM's servers contained trade secrets and intended to steal them in order to harm Plaintiffs.

174. Defendants directly misappropriated Plaintiffs' trade secrets during the hacking of their computer systems and email servers. These trade secrets included confidential business plans, stored on plaintiffs' servers, cost proposals and service projections, information concerning business strategies and opportunities, and contacts for important business relationships.

175. Defendants improperly disclosed and misappropriated Plaintiffs' trade secrets without consent or authorization when they widely disseminated those trade secrets to fellow members of the Qatari Criminal Enterprise, who then distributed them to the media. At the time of such disclosures, Defendants knew or had reason to know that the information disclosed consisted of trade secrets.

176. Defendants misappropriated Plaintiffs' trade secrets intentionally for the benefit their foreign client, Qatar, and acted with the knowledge that their actions would have the effect of benefiting the foreign government of Qatar.

177. As a direct consequence of Defendants' actions, Plaintiffs have suffered damages, which include, but are not limited to, loss of consumer goodwill, loss in the value of Plaintiffs' trade secrets and confidential business information, and harm to Plaintiffs' business, in an amount to be proven at trial. *See* 18 U.S.C. § 1836(b)(3)(B)(i)(I). Defendants' acts of misappropriation have affected interstate commerce.

178. As a direct consequence of Defendants' unlawful actions, Defendants have unjustly benefited from their possession of Plaintiffs' trade secrets. Defendants were paid money by the Qatari Criminal Enterprise to conspire to misappropriate Plaintiffs' trade secrets. Plaintiffs seek damages in the amount of that unjust enrichment, and disgorgement of Defendants' profits pursuant to 18 U.S.C. § 1836(b)(3)(B)(i)(II).

179. Defendants' conduct was willful and malicious, and thus Plaintiffs are entitled to exemplary damages pursuant to 18 U.S.C. § 1836(b)(3)(C), equal to twice the amount of their proven damages. Plaintiffs are also entitled to attorneys' fees pursuant to 18 U.S.C. § 1836(b)(3)(C).

180. Defendants' conduct has caused, and will continue to cause, Plaintiffs irreparable injury, including loss of consumer goodwill, an increased risk of further theft, and an increased risk of harassment. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting Defendants from misappropriating its trade secrets or engaging in any other conduct described in this Cause of Action.

181. Defendants' conduct constitutes criminal conduct in violation of 18 U.S.C. §§ 1831 and 1832. As such, it constitutes predicate racketeering activity under the Racketeer Influenced and Corrupt Organizations ("RICO") Act, 18 U.S.C. § 1962.

COUNT FIVE

Misappropriation of Trade Secrets
Uniform Trade Secrets Act
Cal. Civ. Code § 3426 *et seq.*

182. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

183. The law of the State of California provides a cause of action for damages and injunctive relief in response to the misappropriation of trade secrets. Cal. Civ. Code §§ 3426.2; 3426.3. (While Plaintiffs believe this claim is governed by California law, in the alternative, Plaintiffs hereby allege, based on the same facts, that Defendants have committed misappropriation of trade secrets under New York common law.)

184. Defendants misappropriated a "trade secret" as defined by Cal. Civ. Code § 3426.1 to include "information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

185. The BCM server stored trade secrets, including but not limited to highly confidential business plans and proposals; research supporting those plans and proposals, including cost proposals and service projections; information concerning business strategies and opportunities; and contacts for important business relationships. These trade secrets are of substantial value to Plaintiffs, as will be proven at trial.

186. Moreover, Plaintiffs' emails contained confidential information involving contracts, business proposals, and cost estimates involving Mr. Broidy's company and its clients.

These contracts, proposals, and estimates contained sensitive information about Mr. Broidy's clients and his company's confidential technology and methods.

187. Plaintiffs take and have taken reasonable measures to keep this information secret. For example, Plaintiffs have always maintained their information on secured servers that are protected by passwords, firewalls, and antivirus software.

188. Plaintiffs' trade secrets derive independent actual and potential economic value from not being generally known or available to the public or other persons who can obtain economic value from their disclosure or use.

189. Plaintiffs' trade secrets have significant value, resulting from significant investment of time and resources.

190. Plaintiffs have made, and continue to make, efforts that are reasonable under the circumstances to maintain the secrecy of their trade secrets.

191. Defendants directly misappropriated Plaintiffs' trade secrets by committing and supervising a hack into BCM's computer systems and email servers.

192. Defendants improperly disclosed and misappropriated Plaintiffs' trade secrets without consent or authorization when they widely disseminated those trade secrets to fellow members of the Qatari Criminal Enterprise and to media organizations for publication. At the time of such disclosure, Defendants knew or had reason to know that the information disclosed consisted of trade secrets.

193. As a direct consequence of Defendants' actions, Plaintiffs have suffered damages, which include, but are not limited to, damage resulting from harm to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets and business information, and

other intellectual property; costs expended in protecting trade secrets from future misappropriation; and harm to Plaintiffs' business, in an amount to be proven at trial.

194. As a direct consequence of Defendants' unlawful misappropriation of Plaintiffs' trade secrets, Defendants have unjustly profited from their possession of Plaintiffs' trade secrets. Defendants were paid money from the Qatari Criminal Enterprise to steal and misappropriate Plaintiffs' trade secrets. Plaintiffs seek damages in the amount of that unjust enrichment, and disgorgement of Defendants' profits.

195. Defendants' conduct was willful and malicious, and thus Plaintiffs are entitled to exemplary damages pursuant to Cal. Civ. Code § 3426.3, equal to twice the amount of their proven damages. Plaintiffs are also entitled to attorneys' fees pursuant to Cal. Civ. Code § 3426.4.

196. Defendants' conduct has caused, and will continue to cause, Plaintiffs irreparable injury, including loss of consumer goodwill, an increased risk of further theft, and an increased risk of harassment. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting Defendants from misappropriating its trade secrets or engaging in any other conduct described in this Cause of Action.

COUNT SIX

California Comprehensive Computer Data Access and Fraud Act Cal. Pen. Code § 502

197. California law imposes criminal penalties on anyone who "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network. Cal. Pen. Code § 502(c)(2).

198. California law imposes criminal penalties on anyone who "[k]nowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network." *Id*. § 502(c)(4).

199. California law imposes criminal penalties on anyone who "[k]nowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of" Section 502. *Id*. § 502(c)(6).

200. California law imposes criminal penalties on anyone who "[k]nowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network. *Id.* § 502(c)(7).

201. California law imposes criminal penalties on anyone who "[k]nowingly and without permission uses the Internet domain name or profile of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages or posts and thereby damages or causes damage to a computer, computer data, computer system, or computer network." *Id.* § 502(c)(9).

202. California law provides that "the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access." *Id*. § 502(e)(1).

203. California law provides for award of reasonable attorneys' fees. *Id*. § 502(e)(2).

204. Defendants knowingly and unlawfully accessed computers, computer systems or computer networks at Plaintiff BCM and Google, all of which were located in California. Defendants knew that at the time that they did not have the authorization to access Plaintiffs' computers, computer systems, and networks. This knowledge is demonstrated by conspirators' use of spear phishing attacks and attempted spear phishing attacks to disguise their intentions and obtain login credentials through fraudulent misrepresentations. The spear phishing emails imitated Google's profile in order to obtain login credentials. Defendants caused damage to Plaintiffs electronic files and emails through their cyber intrusions.

205. Defendants knowingly and unlawfully conducted the hacking of BCM's computer systems and email servers, and are therefore directly liable under the Act.

206. As a result of Defendants' actions, Plaintiffs suffered damages, including (without limitation) loss of consumer goodwill; harm to Plaintiffs' computers, servers, and accounts; substantial costs to assess and restore server and digital system security and operations; loss in the value of Plaintiffs' trade secrets, confidential business information, and other intellectual property; and harm to Plaintiffs' business, in an amount to be proven at trial.

207. Defendants' actions were willful and malicious, and Plaintiffs are entitled to punitive damages under § 502(e)(4).

208. Defendants' actions have caused, and will continue to cause, Plaintiffs irreparable injury, including loss of consumer goodwill, an increased risk of further theft, and an increased risk of harassment. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction requiring Defendants to refrain from engaging in any conduct described in this Cause of Action.

COUNT SEVEN

Conversion

209. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

210. Plaintiffs had ownership of and the right to possess their property, including their login credentials, emails, private communications, business documents, trade secrets and intellectual property.

211. By appropriating Plaintiffs' login credentials, Defendants, acting as members of a civil conspiracy and criminal enterprise, unlawfully exercised ownership, dominion, and control over Plaintiffs' electronic documents and emails. They stole a vast amount of valuable electronic information from Plaintiffs' computer systems and email servers, and used them to create PDF and hard-copy documents that they then disseminated to media organizations. Some members of the criminal enterprise, having received stolen property, continued to own and control it, in violation of California Penal Code § 496. Defendants continue to control and disseminate Plaintiffs' emails, electronic communications, business documents, contracts, and intellectual property—included copyrighted materials and trade secrets—and thereby still deny Defendants their lawful dominion, ownership, and control over that property.

212. Defendants' conversion of Plaintiffs' property has caused Plaintiffs to suffer monetary damages, at an amount to be proven at trial, but in any event, in excess of $75,000, exclusive of interest and costs. Plaintiffs' damages include, but are not limited to, damages resulting from injury to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets, confidential business information, and other intellectual property; and harm to Plaintiffs' business, in an amount to be proven at trial. The injury to Plaintiffs is ongoing, and thus the damages Plaintiffs seek are not yet set. Because Defendants' actions are

intolerable in a civilized community, Plaintiffs also seek punitive damages to deter this sort of criminal enterprise behavior.

213. Defendants' massive conversion of such a large amount of Plaintiffs' property has caused, and will continue to cause, Plaintiffs injury, including loss of consumer goodwill, and an increased risk of harassment. Such irreparable harm cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting Defendants from converting or stealing any of Plaintiffs' property, as described in this Cause of Action. Plaintiffs further demand an order requiring Defendants return all stolen property belonging to Plaintiffs immediately upon this Court's order.

COUNT EIGHT

Civil Conspiracy

214. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

215. Defendants agreed to engage in the above-mentioned tortious and criminal actions to harm Mr. Broidy's business and public standing.

216. Defendants willfully, intentionally, and knowingly agreed and conspired with each other and with others, including Qatar and other members of the Qatari Criminal Enterprise, to engage in the wrongful conduct alleged herein, including but not limited to:

(a) Willfully and intentionally accessing without authorization a facility through which an electronic communication service is provided, namely, BCM's computer systems, including its email servers, and thereby obtaining access to wire or electronic communications while they were in electronic storage in such systems, in violation of 18 U.S.C. § 2701(a);

(b) Intentionally accessing Plaintiffs' and Google's servers, and emails and documents physically located on those servers and accounts, without authorization and then stealing and curating Plaintiffs' data and emails, in violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a) and Cal. Pen. Code § 502;

(c) Intentionally, willfully, and without excuse or justification circumventing an access protections on Plaintiffs' copyrighted works, in violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201 *et seq.*;

(d) Willfully, intentionally, and maliciously misappropriating Plaintiffs' trade secrets to benefit the government of Qatar, a foreign power, in violation of both the laws of the United States and California;

(e) Knowingly and intentionally receiving stolen property and concealing that property from Plaintiffs, in violation of California law;

(f) Invading Plaintiffs' privacy by publicizing private facts and intruding upon his seclusion;

(g) Taking and converting Plaintiffs' exclusive private and personal property without permission and with deliberate intent to access and obtain Plaintiffs' personal and private information; and

(h) Tortiously interfering with Plaintiffs' business relationships by using documents and information stolen from Plaintiffs' servers to disparage Plaintiffs' business and conduct.

217. Defendants engaged in numerous overt acts to further conspiracy, including, but not limited to, hacking Plaintiffs' emails and other electronic documents, and hiring subcontractors and other co-conspirators to facilitate the hacking.

218. Defendants each actively participated in the above-described civil conspiracy, and therefore each Defendant is responsible for each tortious and otherwise illegal action of any co-conspirator.

219. As a direct consequence of Defendants' conspiracy, Plaintiffs have suffered monetary damages, at an amount to be proven at trial, but in any event in excess of $75,000, exclusive of interest and costs, which include, but are not limited to, damages resulting from injury to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets, confidential business information, and other intellectual property; and harm to Plaintiffs' business, in an amount to be proven at trial.

220. This conspiracy is ongoing. Defendants' conduct has caused, and will continue to cause, Plaintiffs irreparable injury, including loss of consumer goodwill, an increased risk of further theft, and an increased risk of harassment. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting Defendants from misappropriating its trade secrets or engaging in any other conduct described in this Cause of Action.

COUNT NINE

Violations of RICO Act, 18 U.S.C. § 1962(c) and § 1964

221. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

222. The federal RICO statue provides, "It shall be unlawful for any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or

foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity." 18 U.S.C. § 1962(c).

223. The RICO statute further provides that "Any person injured in his business or property by reason of a violation of section 1962 of this chapter may sue therefor in any appropriate United States district court and shall recover threefold the damages he sustains and the cost of the suit, including a reasonable attorney's fee . . . ." *Id.* § 1964(c).

224. Plaintiffs are "persons" who may sue under Section 1964(c).

225. Defendants are all "persons" subject to the Act.

A. The Qatari Criminal Enterprise is a Separate and Distinct Entity

226. The Qatari Criminal Enterprise is an enterprise under the RICO Act that is distinct from Defendants. It was an association of Qatari officials and hackers (including Defendants), lobbyists and others who worked in common cause to serve Qatar.

227. Through all times relevant to this Complaint, Defendants have associated themselves with the Qatari Criminal Enterprise in fact, although not as a legal entity. Defendants committed the above-described tortious and criminal actions as part of a common purpose to serve the enterprise. These actions were separate and distinct from any legitimate work they performed under contract for Qatar.

228. Upon information and belief, the Qatari Criminal Enterprise consisted of, at least Qatar and its government, Kevin Chalker, Gregory Howard, Nicolas Muzin, Joseph Allaham, Gregory Howard, the Emir of Qatar, and numerous known and unknown individuals, including cyber hackers, public relations professionals, lobbyists, political actors, and others. The criminal enterprise encompassed or corrupted numerous seemingly legitimate institutions and enterprises that provided structure and organization for the enterprise, including but not limited to the Defendant GRA entities, Stonington, and Bluefort Public Relations LLC. All of these

individuals and entities conspired to harm Plaintiffs and did cause them harm through a long-standing pattern of racketeering activity as part of the Qatari Criminal Enterprise.

229. The Qatari Criminal Enterprise engaged in tortious conduct that crossed state lines, spanning from Qatar to California and Washington, DC. Defendants used their interstate media placement and lobbying services to advance the enterprise.

230. Plaintiffs hereby allege and set forth the following predicate racketeering activities as defined under 18 U.S.C. § 1961. Defendants jointly and individually committed each separate set of predicate acts alleged below.

B. First Set of Predicate Acts: Wire Fraud, in violation of 18 U.S.C. § 1343

231. Federal law imposes criminal penalties on "[w]hoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice." 18 U.S.C. § 1343.

232. Defendants as well as their subcontractors, employees, and other co-conspirators intentionally committed numerous acts of wire fraud by obtaining the login credentials of BCM employees through a scheme or artifice—*i.e.*, fake spear phishing emails.

233. At least one such fraudulent email was sent to Robin Rosenzweig. She received an email at her Gmail account that appeared to be a security alert from Google. The email used Google trademarks without the permission of Google, including the Google logo and the Gmail logo. It was sent from a Gmail address and had been disguised to look like an authentic security alert from Google. The email purported to alert Ms. Rosenzweig that the security on her account had been compromised and that she needed to verify or change her account credentials.

234. Defendants used similar spear phishing methods in an unsuccessful attempt to unlawfully access Mr. Mowbray's Google email account.

235. Another such fraudulent spear phishing email was sent to Mr. Broidy's Executive Assistant. These emails were disguised as Google security alerts, which bore Google trademarks used without Google's permission, and were sent through Google's Gmail service in violation of Google's Terms of Service and Gmail's Program Policies.

236. One of the fraudulent spear phishing emails contained a fictitious security alert with a picture of the Executive Assistant's face and part of the Executive Assistant's phone number. The email was sent from a misleading Gmail account with the name "Gmail Account" and the email address noreply.user.secure.services@gmail.com, which had been drafted to look like an authentic security alert from Google. The email purported to alert the Executive Assistant that the security on the account had been compromised and that the Executive Assistant needed to verify or change the Google credentials.

237. Defendants sent numerous spear phishing emails like the ones described above using interstate wires, and these transmissions crossed state lines.

238. Defendants used the spear phishing emails to make material misstatements that induced the targeted individuals to surrender their valuable login credentials.

239. Having fraudulently obtained those credentials through material misstatements, Defendants commenced an illegal cyber-attack against Mr. Broidy and BCM's computer systems and servers. These cyber transmissions used interstate wires and crossed state lines—for example, forensic investigation has revealed that some transmissions traveled from Vermont to California. Defendants and their co-conspirators initiated thousands of intrusions into Plaintiffs' computer systems and email servers.

240. Defendants thereby obtained Plaintiffs' valuable electronic information, including but not limited to emails, private information, contracts, trade secrets, and business plans. Defendants launched the spear phishing attempts with the specific intent of fraudulently depriving Plaintiffs of their valuable property.

241. Defendants each perpetrated several acts of wire fraud by committing and supervising the spear phishing efforts against associates of Mr. Broidy in order to obtain their valuable login credentials to BCM's computer systems and email servers.

242. Defendants' participation in the Qatari Criminal Enterprise began no later than March 2012 and is ongoing.

243. Defendants' tortious scheme targeting Mr. Broidy began in December 2017 and is ongoing.

244. Approximately 1,400 individuals have been victims of wire fraud through cyber hacking by the Qatari Criminal Enterprise, including dozens of American citizens.[8]

245. As a direct consequence of Defendants' actions, Plaintiffs have suffered injury to their business or property, which include, but are not limited to, damage resulting from harm to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets, confidential business information, and other intellectual property; and harm to Plaintiffs' business, in an amount to be proven at trial.

C. Second Set of RICO Offenses: Violations of the Defend Trade Secrets Act. 18 U.S.C. § 1832(a)(1) and (a)(5)

246. The Defend Trade Secrets Act imposes criminal penalties against anyone who "knowingly . . . with intent to convert a trade secret, that is related to a product or service used in

[8] *See* Eli Lake, *supra* n.5.

or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly . . . steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;. . . [or] without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information; [or] receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization." 18 U.S.C. § 1832(a).

247. The Defend Trade Secrets Act also imposes criminal penalties on "whoever . . . conspires with one or more other persons" to violate § 1832(a)(1). *Id*. § 1832(a)(5).

248. Defendants and other members of the Qatari Criminal Enterprise repeatedly violated the Defend Trade Secrets Act, 18 U.S.C. § 1832, *et seq.* The BCM servers stored trade secrets including but not limited to highly confidential business plans and proposals; research supporting those plans and proposals, including cost proposals and service projections; vendor lists; requests for proposals and responses thereto; information concerning business strategies and opportunities; and contacts for important business relationships. BCM is a sophisticated investment management and services firm that possesses and uses its trade secrets to serve its customers and create a competitive market advantage.

249. Moreover, Plaintiffs' emails contained confidential information involving contracts, business proposals, and cost estimates involving Mr. Broidy's company and its clients. These contracts, proposals, and estimates contained sensitive information about Mr. Broidy's clients and his company's confidential technology and methods.

250. These trade secrets are of substantial value to Plaintiffs, and they were used and intended for use in relation to products and services in interstate and foreign commerce.

251. Plaintiffs take and have taken reasonable measures to keep this information secret. For example, Plaintiffs have always maintained their information on secured servers that are protected by passwords, firewalls, and antivirus software.

252. Plaintiffs' trade secrets derive independent actual and potential economic value from not being generally known or available to the public or other persons who can obtain economic value from their disclosure or use.

253. Plaintiffs' trade secrets have significant value, resulting from significant investment of time and resources.

254. Plaintiffs have made, and continue to make, efforts that are reasonable under the circumstances to maintain the secrecy of their trade secrets.

255. Defendants each unlawfully and without authorization appropriated, obtained, and stole Plaintiffs' trade secrets. Defendants knew that BCM's servers contained trade secrets and intended to steal them in order to harm Plaintiffs and economically benefit both themselves and Qatar. Defendants were paid substantial amounts to misappropriate and publish Plaintiffs' trade secrets, and Qatar hoped to use those trade secrets to its economic benefit. Defendants thereby committed multiple violations of the Defend Trade Secrets Act.

256. Defendants' knowing and intentional violation of the Defend Trade Secrets Act has materially injured Plaintiffs. It has deprived them of valuable trade secrets, and caused them to expend resources to defend against further cyber-attacks.

257. The Qatari Criminal Enterprise's misappropriation of Plaintiffs' trade secrets began in January of 2018 and is ongoing.

258. Defendants' actions have caused Plaintiffs to suffer injury to their business or property, including (without limitation) damage resulting from harm to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets, confidential business information; and harm to Plaintiffs' business, in an amount to be proven at trial.

D. Third Set of Predicate Acts: Economic Espionage, in Violation of 18 U.S.C. §§ 1831(a)(1) and (a)(5)

259. Federal law provides that "[w]hoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret . . . [or] (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization" violates 18 U.S.C. § 1831(a)(1).

260. Federal law also imposes penalties on "[w]hoever . . . conspires with one or more other persons to commit" a violation of § 1831(a)(1). *Id*. § 1831(a)(5).

261. Defendants each unlawfully and without authorization took, appropriated, and obtained Plaintiffs' trade secrets through the cyber-attack against Plaintiffs' servers. Defendants and other members of the Qatari Criminal Enterprise knew that BCM's servers contained trade secrets and intended to steal them in order to harm Plaintiffs. They misappropriated Plaintiffs' trade secrets intentionally for the benefit of their foreign client, Qatar, and acted with the knowledge that their actions would have the effect of benefiting the foreign nation of Qatar.

262. Defendants used an artifice and fraud—the fake Gmail spear phishing emails—in order to take, appropriate, and obtain Plaintiffs' trade secrets.

263. Defendants used fake spear phishing emails to induce targets to surrender their valuable login credentials. Multiple targets did provide their login credentials in reliance of these false material statements.

264. As a direct consequence of Defendants' misappropriation, Plaintiffs have suffered injury to their business or property, which include, but are not limited to, damages resulting from harm to Plaintiffs' computers, servers, and accounts, loss in the value of Plaintiffs' trade secrets and business information, and harm to Plaintiffs' business, in an amount to be proven at trial.

E. Fourth Set of Predicate Acts: Criminal Copyright Infringement, in Violation of 17 U.S.C. § 506(a)(1)

265. Federal law provides that "[a]ny person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed . . . for purposes of commercial advantage or private financial gain." 17 U.S.C. § 506.

266. Plaintiffs' computer systems and email servers contained numerous copyrighted works protected under federal law, including Plaintiffs' emails and their contents.

267. Defendants conducted and supervised the misappropriation of Plaintiffs' numerous copyrighted works through the hacking. They therefore each committed multiple predicate acts of criminal copyright infringement.

268. Defendants hacked into Plaintiffs' computer systems and email servers. Defendants then violated Plaintiffs' copyright on those materials by indiscriminately copying them, and reproducing some of them in PDF form, and distributing them to the media.

269. Defendants' violation of Plaintiffs' copyright was intentional and willful.

270. Plaintiffs' copyrighted material was valuable, and Defendants illicitly obtained that value by stealing and reproducing Plaintiffs' copyrighted works.

271. Defendants violated Plaintiffs' copyright for purposes of commercial advantage or private financial gain. Defendants sought to harm Plaintiffs financially in order to silence Mr. Broidy, and thereby gain a commercial advantage in the form of eased sanctions. Moreover, Defendants were paid by the Qatari Criminal Enterprise to violate Plaintiffs' copyright.

272. As a direct consequence of Defendants' criminal copyright violations, Plaintiffs have suffered injury to their business and property, which include, but are not limited to, damages resulting from injury to Plaintiffs' value in their copyrighted information, in an amount to be proven at trial.

F. Pattern of Racketeering Activity

273. The Qatari Criminal Enterprise has engaged in a pattern of racketeering activity with relationship and continuity. More than one thousand individuals, many critics of Qatar and its allies, have been victimized by the criminal enterprise's cyber-attacks since March 2012 at the latest. These tortious actions form a related pattern because the enterprise committed the aforementioned racketeering activity for a common purpose: to silence Qatar's critics. Thus, the Qatari Criminal Enterprise has perpetrated multiple schemes, inflicting numerous injuries against many victims over a substantial amount of time. The scheme against Plaintiffs in particular extended from, at the latest, September 2017 and extended through the dissemination of Plaintiffs' stolen documents to the media, which continued to publish harmful articles about Mr. Broidy throughout 2018 and to the present day. Thus, the Qatari Criminal Enterprise has committed a "closed-ended" scheme of racketeering violations lasting well over a year.

274. Defendants each engaged in at least two predicate acts of racketeering. Defendants are each directly and primarily liable for multiple acts of wire fraud, misappropriation of trade secrets, economic espionage, and criminal copyright infringement.

275. Specifically, Defendants each committed thousands of instances of wire fraud, with each intrusion into Plaintiffs' computer systems and email servers constituting a separate predicate act committed by each Defendant. Defendants also committed multiple predicate acts of wire fraud by transmitting several phony spear phishing emails and other fraudulent communications to Robin Rosenzweig, Mr. Broidy's Executive Assistant, and Joel Mowbray. Defendants each committed numerous predicate acts of misappropriation of trade secrets, with each misappropriated business plan, cost and service projection, contract, or other trade secret constituting a separate predicate act. Because Defendants misappropriated Plaintiffs' trade secrets for the benefit of Qatar, they are also each liable for multiple acts of Economic Espionage. Finally, Defendants committed numerous acts of criminal copyright infringement by unlawfully opening, reading, transmitting, and then transmitting Plaintiffs' emails, many of which contained copyrightable material, to fellow co-conspirators. In sum, each Defendant committed thousands of separate predicate acts, and the precise number will be proven at trial.

276. Moreover, the Qatari Criminal Enterprise's campaign to silence its critics is ongoing, and it continues to commit acts of racketeering to shield Qatar from public scrutiny. Media organizations are still to this day relying on information stolen from Mr. Broidy's computer systems and email servers to publish stories to damage his image. For example, media outlets have continued to falsely claim that Mr. Broidy was a target in the investigation of special counsel Robert Mueller into Russian interference in U.S. elections, whereas in reality he was never contacted by Mueller's team and does not appear once in the Mueller Report. The enterprise has thus also engaged in an "open-ended" scheme of racketeering. If left unchecked, the Qatari Criminal Enterprise presents a distinct threat of long-term racketeering activity.

G. Defendants Exercised Management and Operation of the Enterprise

277. Defendants operated and managed the affairs of the Qatari Criminal Enterprise and in particular implemented the cyber-attacks against Plaintiffs and coordinated and helped execute its media disinformation campaign against Plaintiffs. Initially Defendants oversaw a complex, international project to silence and otherwise neutralize the critics of Qatar's 2022 World Cup bid. The enterprise delegated the cyber-attack against Mr. Broidy to Defendants, who used their expertise in offensive cyber operations and espionage to hire subcontractors and individual hackers, organize the cyber intrusions, and send the spear phishing emails that would illegally obtain login credentials to BCM's computer systems and email servers. They managed and directed the activities of sophisticated hackers and cyber-firms. They had substantial decision-making authority and discretion to conduct the cyber-attack on Plaintiffs.

H. Effect on Interstate Commerce

278. The Qatari Criminal Enterprise has substantially affected interstate commerce by, for example, harming Plaintiffs' property and business, including but not limited to loss to and consumer goodwill and loss of valuable electronic information, business plans, contracts, vendor lists, requests for proposals, copyrighted materials, and substantial expense in protecting Plaintiffs' computer systems and email servers from additional cyber-attack. Plaintiffs regularly conduct business in interstate commerce, and Defendants' cyber-hacking has substantially disturbed that business.

I. Business Injury

279. As a direct consequence and by reason of Defendants' racketeering activity, Plaintiffs have suffered injury to their business and property, which includes, but is not limited to, financial damage resulting from loss of consumer goodwill and business relationships; damage to Plaintiffs' computers, servers, and accounts; loss caused by the investigation of the

hackings and the securing of Plaintiffs' systems against further intrusions; lost profits; and loss in the value of Plaintiffs' trade secrets, confidential business information, and other intellectual property, in an amount to be proven at trial. Plaintiffs also lost existing business relationships because customers and potential business partners were concerned about the security of their data following the cyber-attack. Plaintiffs' trade secrets, copyrightable material, and other confidential information are valuable property, and the harm inflicted on their relationships with customers and business partners constitute a distinct set of business injuries.

280. Plaintiffs' injuries were factually and proximately caused by Defendants' acts of racketeering. The harm to Plaintiffs' computer, servers, accounts, as well as the misappropriation of the trade secrets, copyrighted materials, and other confidential information contained on them, was readily foreseeable, and indeed intended by Defendants and their fellow co-conspirators in the Qatari Criminal Enterprise. The harm to Plaintiffs' relationships with customers and potential business partners was likewise a natural and foreseeable result of Defendants' offensive cyber-attacks and related racketeering activity. In particular, the hacking left the false impression with Plaintiffs' customers and potential business partners that Plaintiffs had not reasonably secured the data contained in their computer systems and email servers..

281. Moreover, the central goal of the hacking was to obtain documents that would then be carefully curated and disseminated to cooperative members of the media for publication. These stories attempted to tie Mr. Broidy to wrongful conduct, and thereby, as Mr. Muzin stated to Mr. Allaham, put Plaintiffs "in Mueller's crosshairs" and "make Broidy go away altogether." Thus, the injuries caused by the publication of numerous damaging stories about Plaintiffs were also foreseeable and traceable to Defendants' racketeering conduct.

282. Plaintiffs are entitled to treble damages and attorneys' fees under 18 U.S.C. § 1964(c).

COUNT TEN

Conspiracy to Violate RICO Statute, 18 U.S.C. § 1962(d)

283. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

284. The RICO Act provides that "[i]t shall be unlawful for any person to conspire to violate any of the provisions" of the Act. 18 U.S.C. § 1962(d).

285. Defendants knowingly and voluntarily agreed with other members of the Qatari Criminal Enterprise to engage in the above-mentioned racketeering actions to harm Mr. Broidy's business and standing in the community. Defendants agreed to participate in the conspiracy at the very latest before opening an office in Doha, Qatar in October 2017.

286. Defendants and other members of the Qatari Criminal Enterprise committed the above-referenced racketeering acts in furtherance of their racketeering conspiracy.

287. Defendants each committed numerous acts of racketeering in furtherance of the conspiracy, including wire fraud, misappropriation of trade secrets, economic espionage, and criminal copyright infringement.

288. As a direct consequence and by reason of Defendants' racketeering conspiracy, Plaintiffs have suffered injury to their business and property, which includes, but is not limited to, damage resulting from loss of consumer goodwill; harm to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets, confidential business information, and other intellectual property; and harm to Plaintiffs' business, in an amount to be proven at trial. These injuries to Plaintiffs' business and property were the natural, foreseeable, and intended result of Defendants' RICO conspiracy and the acts committed in furtherance thereof.

289. Plaintiffs are entitled to treble damages and attorneys' fees under 18 U.S.C. § 1964(c).

PRAYER FOR RELIEF

290. Plaintiffs repeat and re-allege the allegations contained in each and every preceding paragraph of this Complaint.

291. Wherefore, Plaintiffs request that this Court order the following relief against Defendants:

(a) Grant judgment in favor of Plaintiffs and against Defendants as to all Causes of Action;

(b) Declare that Defendants' conduct constitutes violations of the statutes and common law cited herein;

(c) Award Plaintiffs an appropriate amount in monetary damages as determined at trial, including but not limited to pre- and post-judgment interest and treble damages under RICO, 18 U.S.C. § 1964 and Cal. Pen. Code § 496;

(d) Grant all appropriate injunctive relief against Defendants, disgorgement of unjust riches, constructive trust over Plaintiffs' trade secrets and other materials, and any other equitable relief deemed appropriate;

(e) Award Plaintiffs punitive damages under 18 U.S.C. § 2707, and Cal. Pen. Code § 502, and Plaintiffs' common-law causes of action, as well as exemplary damages under Cal. Civ. Code § 3426.3, and 18 U.S.C. § 1836(b)(3)(C);

(f) Award Plaintiffs attorneys' fees and the costs of bringing this action; and

(g) Grant Plaintiffs such other relief as is just and appropriate.

JURY DEMAND

Plaintiffs hereby demand a trial by jury.

Respectfully Submitted,

STEPTOE & JOHNSON LLP

/s/ Filiberto Agusti
Filiberto Agusti
1330 Connecticut Avenue, NW
Washington, DC 20036
Phone: (202) 429-3000
Fax: (202) 429-3902
fagusti@steptoe.com

Charles Michael
1114 Avenue of the Americas
New York, NY 10036
Phone: (212) 506-3900
Fax: (202) 506-3950
cmichael@steptoe.com

Counsel for Plaintiffs Elliott Broidy and Broidy Capital Management LLC

Dated: December 27, 2019